RE: Vulnerabilitate - Sistem Formulare ISBN (Posibil altele)

"Cristian Cojan" <cristian.cojan@bibnat.ro>
September 7, 2023 at 12:53 PM
To: office@incorpo.ro
Cc: bitt@bibnat.ro, secretariat@bibnat.ro

Buna ziua,

Am sters acel fisier.

In viitorul foarte apropiat site-ul bibliotecii va fi schimbat, iar cel actual va fi retras.

Vom tine cont in constructia noului site de aceste tipuri de vulnerabilitati.

Va multumumim pentru informatiile pe care ni le-ati transmis.

Cu stima,

Cristian Cojan

From: office@incorpo.ro [mailto:office@incorpo.ro]
Sent: Thursday, September 7, 2023 11:58 AM
To: bitt@bibnat.ro; secretariat@bibnat.ro
Subject: Vulnerabilitate - Sistem Formulare ISBN (Posibil altele)

Buna ziua,

Va contactez in legatura cu o vulnerabilitate la formularul de transmitere a informatiilor de pe pagina bibnat.ro, care permite actorilor maliciosi uploadarea de fisiere arbitrare, inclusiv fisiere care pot fi executate de catre serveurl web (Fisiere php).

In lipsa unui sistem de sanitizare a documentelor uploadate ca pagina de titlu, actorii maliciosi pot incarca orice fel de fisier, de la fisiere non-imagine (sau .pdf), la fisiere .php, .aspx, etc, care pot genera riscul de a putea deveni executabile.

Exemplu fisier .php executabil uploadat, care permite executia arbitrara de comenzi si accesul la fisierele din web root: https://www.bibnat.ro/documente/dynforms/doc_169407556648924947.php

Va rugam vehement ca dupa validarea vulnerabilitatii, sa stergeti fisierul .php, pana la solutionarea problemei (sau pastrarea lui in afara serverului web, pentru a testa validitatea rezolvarii problemei).

Codul original este accesibil aici: https://github.com/flozz/p0wny-shell

Fisiere Afectate:

- sectiune.php#formular (Probabil persista in mai multe fisiere) de pe platforma web.

Pentru a reproduce problema, se poate accesa "https://www.bibnat.ro/ISBN-s21-ro.htm", incarca un fisier arbitrar (eg: .php), si deschiderea link-ului primit prin e-mail.

De asemenea, in contextul aparitiei unei erori la accesarea directa a endpoint-ului de formular, exista riscul sa existe, suplimentar, si o vulnerabilitate de SQL injection, care ar permite atacatorilor accesul la toate tabelele si bazele de date pentru care utilizatorul care executa acele query-uri are acces. (Cand este accesat cu GET request)

Solutii pe termen scurt:

- Dezactivarea executarii de orice fel de script (.php, .aspx, etc) in folder-urile unde se uploadeaza fisiere.
- Dezactivarea executarii de programe de catre php, pentru a preveni functionalitatea tool-urilor de web shell.

Solutii pe termen lung:

- Identificarea tuturor formularelor de natura sa nu sanitizeze marimea, tipul, mimeType-ul, etc al fisierelor uploadate, si blocarea acestora, impreuna cu implementarea solutiilor pe termen scurt.
- Tranzitia la un sistem open-source gratuit, pentru a nu fi necesara supra-alocarea de resurse spre mentinerea si updatarea platformei dezvoltata intern (Ghost CMS, Wordpress, etc)

Va stam la dispozitie pe E-Mail, precum si telefonic, pentru orice intrebare referitoare la problema semnalata. De asemenea, ne oferim disponibilitatea de a asista, cu titlu gratuit, la solutionarea problemei.

Multumesc,

Incorpo.Ro Logo

Deleanu Stefan-Lucian
Director / ENTRYRISE S.R.L

Website: www.incorpo.ro
Email: office@incorpo.ro
Phone: +40786833325